

# ELLIPTIC CURVES WITH MAXIMALLY DISJOINT DIVISION FIELDS

HARRIS B. DANIELS, JEFFREY HATLEY, AND JAMES RICCI

**ABSTRACT.** One of the many interesting algebraic objects associated to a given rational elliptic curve,  $E$ , is its full-torsion representation  $\rho_E : \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow \text{GL}_2(\hat{\mathbf{Z}})$ . Generalizing this idea, one can create another full-torsion Galois representation,  $\rho_{(E_1, E_2)} : \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow (\text{GL}_2(\hat{\mathbf{Z}}))^2$  associated to a pair  $(E_1, E_2)$  of rational elliptic curves. The goal of this paper is to provide an infinite number of concrete examples of pairs of elliptic curves whose associated full-torsion Galois representation  $\rho_{(E_1, E_2)}$  has maximal image. The size of the image is inversely related to the size of the intersection of various division fields defined by  $E_1$  and  $E_2$ . The representation  $\rho_{(E_1, E_2)}$  has maximal image when these division fields are maximally disjoint, and most of the paper is devoted to studying these intersections.

## 1. INTRODUCTION

Let  $E$  be an elliptic curve defined over  $\mathbf{Q}$ , let  $\bar{\mathbf{Q}}$  be a fixed algebraic closure of  $\mathbf{Q}$ , and for each positive integer  $n$  let

$$E[n] = \{P \in E(\bar{\mathbf{Q}}) : [n]P = \mathcal{O}\}$$

denote the  $n$ -torsion of  $E$ . It is a classical result that  $E[n]$  is non-canonically isomorphic to  $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$  and the group  $G_{\mathbf{Q}} = \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$  acts on  $E[n]$  component-wise. Therefore, we can construct a Galois representation associated to the  $n$ -torsion of  $E$ ,

$$\bar{\rho}_{E,n} : G_{\mathbf{Q}} \rightarrow \text{Aut}(E[n]) \simeq \text{GL}_2(\mathbf{Z}/n\mathbf{Z}).$$

By choosing compatible bases and taking an inverse limit ordered by divisibility, we can construct the full-torsion representation associated to  $E$ ,

$$\rho_E : G_{\mathbf{Q}} \rightarrow \text{GL}_2(\hat{\mathbf{Z}}) \simeq \prod_p \text{GL}_2(\mathbf{Z}_p),$$

where the product is taken over all prime numbers.

A natural question is, how large can the image of  $\rho_E$  be inside of  $\text{GL}_2(\hat{\mathbf{Z}})$ ? More specifically, can  $\rho_E$  be surjective? With these questions in mind, we give the following definition:

**Definition 1.1.** An integer  $n \geq 2$  is said to be *exceptional* for  $E$  if  $\bar{\rho}_{E,n}$  is not surjective.

We can translate questions about the size of  $\text{Im } \rho_E$  into a question about which numbers are exceptional for  $E$  and, for an exceptional  $n$ , how drastically  $\rho_{E,n}$  fails to be surjective. It is a standard result that when  $E$  is an elliptic curve with complex multiplication (CM), *every* integer except for possibly 2 is exceptional for  $E$ . See [10, Theorem 2.3] for more detail. On the other hand, if  $E$  is a rational elliptic curve that does not have CM, Serre showed in [8] that the index  $[\text{GL}_2(\hat{\mathbf{Z}}) : \text{Im } \rho_E]$  is finite. One implication of this is that for each elliptic curve there are only finitely many exceptional primes. Additionally, Serre proved the following theorem.

---

*Date:* July 28, 2015.

1991 *Mathematics Subject Classification.* Primary 14H52; Secondary 11F80.

*Key words and phrases.* Elliptic Curves, Galois Representations.

**Proposition 1.2.** [8, Proposition 22] *For any elliptic curve  $E$  defined over  $\mathbf{Q}$ , the image of  $\rho_E : G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\widehat{\mathbf{Z}})$  is contained in a group of index 2 inside  $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ .*

This theorem implies that  $\rho_E$  can never be surjective, and thus there exists at least one exceptional number  $n$  (not necessarily prime). In the same paper, Serre gave two examples of elliptic curves whose image has index exactly 2 inside  $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ , showing that this lower bound on the index of  $\mathrm{Im} \rho_E$  is sharp.

Following Lang and Trotter we give the following definition:

**Definition 1.3.** An elliptic curve  $E/\mathbf{Q}$  is called a **Serre curve** if  $[\mathrm{GL}_2(\widehat{\mathbf{Z}}) : \mathrm{Im} \rho_E] = 2$ .

Furthermore, there is no reason to restrict our attention to Galois representations associated to only *one* elliptic curve. Given a pair of rational elliptic curves  $(E_1, E_2)$  and a positive integer  $n$ , we can consider the action of  $G_{\mathbf{Q}}$  on  $E_1[n] \times E_2[n]$  to get a new Galois representation

$$\bar{\rho}_{(E_1, E_2), n} : G_{\mathbf{Q}} \rightarrow (\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}))^2,$$

given by  $\bar{\rho}_{(E_1, E_2), n}(\sigma) = (\bar{\rho}_{E_1, n}(\sigma), \bar{\rho}_{E_2, n}(\sigma))$ . Just as before we can construct the full-torsion representation associated to the pair  $(E_1, E_2)$

$$\rho_{(E_1, E_2)} : G_{\mathbf{Q}} \rightarrow (\mathrm{GL}_2(\widehat{\mathbf{Z}}))^2,$$

and it is again natural to ask, how big can the image of  $\rho_{(E_1, E_2)}$  be?

There is a natural limitation on the size of the image of  $\rho_{(E_1, E_2)}$  in  $\mathrm{GL}_2(\widehat{\mathbf{Z}})$  coming from the Weil pairing. Given an elliptic curve  $E/\mathbf{Q}$ , let  $\mathbf{Q}(E[n])$  be the field of definition of the  $n$ -torsion points of  $E$ . One consequence of the Weil pairing is that if  $\zeta_n$  is a primitive  $n$ -th root of unity, then  $\mathbf{Q}(\zeta_n) \subset \mathbf{Q}(E[n])$ . Therefore, it must be that  $\mathbf{Q}(\zeta_n) \subset \mathbf{Q}(E_1[n]) \cap \mathbf{Q}(E_2[n])$ .

The action of an element in the Galois group on an  $n$ -th root of unity can be related to its image under  $\bar{\rho}_{E, n}$  through the determinant. That is, given an elliptic curve  $E/\mathbf{Q}$ ,  $\sigma \in G_{\mathbf{Q}}$ , and an  $n$ -th root of unity  $\zeta_n$ , it must *always* be that

$$(1.1) \quad \sigma(\zeta_n) = \zeta_n^{\det(\bar{\rho}_{E, n}(\sigma))}.$$

Therefore, for each positive integer  $n$ , we define

$$D_n := \left\{ (A, B) \in (\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}))^2 : \det A = \det B \right\}$$

and

$$D := \left\{ (A, B) \in (\mathrm{GL}_2(\widehat{\mathbf{Z}}))^2 : \det A = \det B \right\}.$$

With these definitions and the observations above we can see that for any pair of rational elliptic curves  $(E_1, E_2)$  and positive integer  $n$ , the image of  $\bar{\rho}_{(E_1, E_2), n}$  and  $\rho_{(E_1, E_2)}$  must be contained inside of  $D_n$  and  $D$  respectively. Therefore, any result associated with the size of  $\mathrm{Im} \rho_{(E_1, E_2)}$  should be formulated in terms of  $[D : \mathrm{Im} \rho_{(E_1, E_2)}]$ .

For any two elliptic curves  $E_1$  and  $E_2$  defined over  $\mathbf{Q}$ , we have

$$\mathrm{Im} \rho_{(E_1, E_2)} \subset (\mathrm{Im} \rho_{E_1} \times \mathrm{Im} \rho_{E_2}) \cap D.$$

Since the right-hand side has index at least 4 inside of  $D$  (by Proposition 1.2), we give the following definition in the spirit of Definition 1.3:

**Definition 1.4.** A pair  $(E_1, E_2)$  is called a **Serre pair** if  $[D : \mathrm{Im} \rho_{(E_1, E_2)}] = 4$ .

In [4], Jones shows that, in some appropriate sense, almost all pairs of elliptic curves are Serre pairs. The proof uses a multi-dimensional large sieve but provides no concrete examples of Serre pairs. In fact, there are no examples of Serre pairs in the current literature. The main goal of this paper is to rectify this deficiency by providing infinitely many examples of

Serre pairs. The first step toward this goal is to find an infinite family of Serre curves since clearly any Serre pair must be a pair of Serre curves.

**Lemma 1.5.** [2, Example 8.2] *Let  $\ell$  be an odd prime with  $\ell \neq 7$ . Then the elliptic curve*

$$E_\ell : y^2 + xy = x^3 + \ell$$

*is a Serre curve.*

Using this lemma we will be able to construct the first examples of Serre pairs coming from the main theorem of this paper:

**Theorem 1.6.** *Let  $\ell_1$  and  $\ell_2$  be odd primes not equal to 7 such that  $\gcd(432\ell_1^2 + \ell_1, 432\ell_2^2 + \ell_2) = 1$ , and for  $i = 1, 2$  let*

$$E_{\ell_i} : y^2 + xy = x^3 + \ell_i.$$

*Then the pair  $(E_{\ell_1}, E_{\ell_2})$  is a Serre pair.*

In fact, we obtain the following slightly stronger result.

**Corollary 1.7.** *Let  $\ell_1$  be an odd prime different from 7. Then there exist infinitely many primes  $\ell_2$  such that the pair  $(E_{\ell_1}, E_{\ell_2})$  is a Serre pair.*

PROOF: Let  $\Delta = 432\ell_1^2 + \ell_1$  and suppose it factors as  $\Delta = p_1^{e_1} \cdots p_n^{e_n}$ . By Theorem 1.6, it suffices to show that there exist infinitely many primes  $\ell_2 \nmid \Delta$  such that

$$432\ell_2 + 1 \not\equiv 0 \pmod{p_i} \text{ for every } i = 1, \dots, n.$$

First notice that if  $\ell_1 = 3$ , then by Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many primes  $\ell_2$  different from 3 and 1297 such that  $\ell_2 \not\equiv 3 \pmod{1297}$ .

Otherwise, if  $\ell_1 \neq 3$ , then  $432\ell_1 \equiv -1$  is a unit modulo  $\Delta$  and since each  $p_i \mid \Delta$ , we have

$$432\ell_2 + 1 \equiv 0 \pmod{p_i} \implies \ell_2 \equiv \ell_1 \pmod{p_i}.$$

Therefore, it suffices to show that there are infinitely many  $\ell_2$  such that  $\ell_2 \not\equiv \ell_1 \pmod{p_i}$  for all  $1 \leq i \leq n$ . By the Chinese remainder theorem, we can choose  $x$  such that  $x \not\equiv 0, \ell_1 \pmod{p_i}$  for each  $i$ . An application of Dirichlet's theorem on the sequence  $\{x + (p_1 \cdots p_n)k\}_{k \in \mathbb{N}}$  then guarantees the existence of infinitely many primes  $\ell_2$  with the desired property. ■

**Remark 1.8.** The quantity  $432\ell_i^2 + \ell_i$  is the discriminant of the elliptic curve  $E_i$ . As we discuss below in Proposition 2.2 and Lemma 2.3, the hypothesis that  $\gcd(432\ell_1^2 + \ell_1, 432\ell_2^2 + \ell_2) = 1$  imposes constraints on the ramification in the division fields associated to our elliptic curves.

In order to prove this theorem we will need the following lemma:

**Lemma 1.9.** *Let  $(E_1, E_2)$  be a pair of rational elliptic curves. If*

- (1) *for each prime  $p \geq 5$ ,  $\text{Im } \bar{\rho}_{(E_1, E_2), p} = D_p$ , and*
- (2)  *$\text{Im } \bar{\rho}_{(E_1, E_2), 36} = D_{36}$ ,*

*then  $(E_1, E_2)$  is a Serre Pair.*

PROOF: This follows immediately from [4, Lemma 3.1]. ■

Lemma 1.9 gives us two concrete conditions that we use to verify our pairs of elliptic curves are in fact Serre pairs.

**1.1. Notation and Outline.** Throughout the rest of this paper, fix two odd primes  $\ell_1$  and  $\ell_2$ , both different from 7, such that  $\gcd(432\ell_1^2 + \ell_1, 432\ell_2^2 + \ell_2) = 1$ . For  $i = 1, 2$  we will write

$$E_i : y^2 + xy = x^3 + \ell_i.$$

Then by Lemma 1.5,  $E_1$  and  $E_2$  are both Serre curves. In particular, as explained in [2], we have that

$$\bar{\rho}_{E_i, p^n} : G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$$

is surjective for every prime  $p$  and every integer  $n \geq 1$ .

Our strategy is to use Lemma 1.9 to prove that  $(E_1, E_2)$  is a Serre pair. Thus, our paper divides naturally into two main sections: a study of  $\bar{\rho}_{(E_1, E_2), p}$  for all primes  $p \geq 5$ , and a separate study of  $\bar{\rho}_{(E_1, E_2), 36}$ . In both cases, we interpret the conditions of Lemma 1.9 in terms of the Galois theory of the division fields associated to the Serre curves  $E_i$ . Let  $K_i = \mathbf{Q}(E_i[p^n])$  denote the Galois number field obtained by adjoining to  $\mathbf{Q}$  the coordinates of the  $p^n$ -torsion points of  $E_i$ . The Weil pairing forces the intersection  $K_1 \cap K_2$  to be a non-trivial extension of  $\mathbf{Q}$ ; in particular, the intersection contains the  $p^n$ -cyclotomic field  $\mathbf{Q}(\zeta_{p^n})$ . The main results of this paper state that, apart from the cyclotomic subextension, the division fields  $K_1$  and  $K_2$  are maximally disjoint for all primes  $p$  and all integers  $n \geq 1$ . Theorem 1.6 then follows directly from the conditions found in Lemma 1.9.

## 2. $p$ -DIVISION FIELDS FOR $p \geq 5$

For the entirety of this section fix a prime  $p \geq 5$  and, since  $\ell_1 \neq \ell_2$ , assume without loss of generality that  $p \neq \ell_1$ . Let  $K_i = \mathbf{Q}(E_i[p])$  denote the number field obtained by adjoining to  $\mathbf{Q}$  the  $x$ - and  $y$ -coordinates of the  $p$ -torsion points of  $E_i$ . Since  $E_i$  is a Serre curve, we have

$$\mathrm{Gal}(K_i/\mathbf{Q}) \simeq \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}).$$

As explained in the introduction, the Weil pairing forces the inclusion  $\mathbf{Q}(\zeta_p) \subset K_i$ , where  $\zeta_p$  denotes a primitive  $p$ -th root of unity and  $\mathbf{Q}(\zeta_p)$  denotes the  $p$ -cyclotomic extension of  $\mathbf{Q}$ . Let  $F = K_1 \cap K_2$  denote the intersection of the two division fields; then  $F \supset \mathbf{Q}(\zeta_p)$  is strictly larger than  $\mathbf{Q}$ .

Recall that condition (1) of Lemma 1.9 states the following:

$$(2.1) \quad \mathrm{Im} \bar{\rho}_{(E_1, E_2), p} = D_p, \text{ where } D_p = \left\{ (A, B) \in \left( \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}) \right)^2 : \det A = \det B \right\}$$

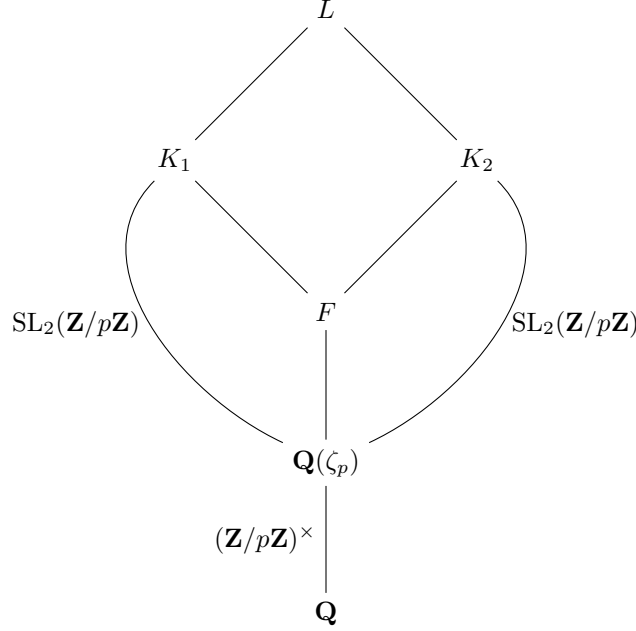
This condition can be interpreted using the Galois theoretic properties of the  $K_i$ , as we now describe.

First, recall that the determinant of  $\bar{\rho}_{E_i, p}$  is the cyclotomic character  $\chi_p$ , which cuts out the cyclotomic extension  $\mathbf{Q}(\zeta_p)/\mathbf{Q}$  via the canonical isomorphism  $\chi_p : \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^\times$ .

Now let  $L = K_1 K_2$  denote the compositum of the division fields. Then  $\mathrm{Gal}(L/\mathbf{Q})$  is a subgroup of the direct product  $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}) \times \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$ . Since the intersection  $F$  is a nontrivial extension of  $\mathbf{Q}$ ,  $\mathrm{Gal}(L/\mathbf{Q})$  must be a *proper* subgroup. The following result is well-known.

**Lemma 2.1** (Goursat's Lemma). *Let  $G_1$  and  $G_2$  be groups, and let  $H$  be a subgroup of the direct product  $G_1 \times G_2$  such that the natural projections  $\pi_1 : H \rightarrow G_1$  and  $\pi_2 : H \rightarrow G_2$  are surjective. Let  $N_1$  denote the kernel of  $\pi_2$  and  $N_2$  denote the kernel of  $\pi_1$ . Then regarding  $N_i$  as a subgroup of  $G_i$ , the image of  $H$  in  $G_1/N_1 \times G_2/N_2$  is the graph of an isomorphism  $G_1/N_1 \simeq G_2/N_2$ .*

PROOF: See [7, Lemma 5.2.1]. ■


 FIGURE 1. Division fields for  $p \geq 5$ 

Write  $G_i = \mathrm{Gal}(K_i/\mathbf{Q})$ , and for the moment let  $H = \mathrm{Gal}(L/\mathbf{Q})$ . Goursat's lemma shows that  $H$  is a certain fibered product of  $G_1$  and  $G_2$ . Furthermore, since we have  $G_1 \simeq G_2 \simeq \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$ ,  $H$  is determined by a unique normal subgroup  $N$  of  $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$ . For example, if  $H$  were equal to the entire direct product  $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}) \times \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$ , then we would have  $N = \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$ , and the common fixed field  $F = K_1 \cap K_2$  would be equal to  $\mathbf{Q}$ .

Goursat's lemma thus gives the following Galois-theoretic interpretation of (2.1): since  $\det \bar{\rho}_{E_i, p} = \chi_p$  cuts out  $\mathbf{Q}(\zeta_p)$ , we have

$$\mathrm{Im} \bar{\rho}_{(E_1, E_2), p} = D_p \iff F = \mathbf{Q}(\zeta_p).$$

So (2.1) is equivalent to the statement that  $H$  is the fibered product of  $G_1$  and  $G_2$  over  $\mathbf{Q}(\zeta_p)$ , which is equivalent to  $K_1$  and  $K_2$  being maximally disjoint. Our goal is now to show that  $F = \mathbf{Q}(\zeta_p)$ .

To that end, let us now set  $H := \mathrm{Gal}(L/\mathbf{Q}(\zeta_p))$ . Figure 1 illustrates the associated field diagram with edges labeled by Galois groups.

$H$  is a subgroup of the direct product  $\mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z}) \times \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$ , and we wish to show that  $H \simeq (\mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z}))^2$ . Since  $E_1$  and  $E_2$  are Serre curves, the natural projections  $H \rightarrow \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$  are surjective, and Goursat's lemma implies that  $H$  is determined by a normal subgroup  $N \triangleleft \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$ . As in our previous discussion, we will have  $F = \mathbf{Q}(\zeta_p)$  precisely if  $N = \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$ .

Before proving the main result of this section, we collect some lemmas on the ramification behavior of primes in the  $K_i$ . One computes that  $E_{\ell_i} : y^2 + xy = x^3 + \ell_i$  has discriminant

$$\Delta(E_{\ell_i}) = -\ell_i(432 + \ell_i).$$

Recall that the only primes of bad reduction for  $E_i$  are those dividing  $\Delta(E_i)$ . The following result states that these are also the only primes other than  $p$  which may ramify in  $K_i/\mathbf{Q}$ .

**Proposition 2.2** (Neron, Ogg, Shafarevich). *Let  $E$  be an elliptic curve over  $\mathbf{Q}$ , and let  $p$  be a rational prime. Then the following assertions are equivalent:*

- $E$  has good reduction modulo  $p$ .
- $p$  is unramified in  $\mathbf{Q}(E[n])/\mathbf{Q}$  for all integers  $n \geq 1$  with  $\gcd(n, p) = 1$ .

PROOF: See [9, VII. Theorem 7.1] ■

By hypothesis we have  $\gcd(\Delta(E_1), \Delta(E_2)) = 1$ , so  $\ell_2$  does not ramify in  $K_1$ . The next lemma gives a lower bound on the ramification of  $\ell_1$  in  $K_1$ .

**Lemma 2.3.** *Let  $e_{\ell_i}$  denote the ramification index of  $\ell_i$  in  $K_i/\mathbf{Q}$ . Then  $e_{\ell_i} \geq p$ .*

PROOF: This is worked out in detail in [5, Section 3.2] using the theory of Tate curves. For the proof, we drop the  $i$  subscripts and write simply  $E = E_i$  and  $\ell = \ell_i$ . First, note that the discriminant of  $E$  is

$$\Delta(E) = -\ell(432 + \ell).$$

In particular, the  $\ell$ -adic valuation of  $\Delta(E)$  is

$$\nu_{\ell}(\Delta(E)) = \begin{cases} 1 & \text{if } \ell \neq 3 \\ 2 & \text{if } \ell = 3 \end{cases}$$

and  $E$  has bad (split multiplicative) reduction at  $\ell$ . Our elliptic curve has  $j$ -invariant  $j_E = \frac{1}{\Delta(E)}$ , so in the notation of [5] we have  $\alpha_{\ell} = \nu_p(-\nu_{\ell}(j_E)) = 0$ . By displayed equations (3.4)–(3.7) of [5, Section 3.2], we have

$$e_{\ell} = \begin{cases} (p-1)p & \text{if } p = \ell, \\ p & \text{if } p \neq \ell \end{cases}.$$

Thus, in either case we have  $e_{\ell} \geq p$ . ■

We are now prepared to prove the following.

**Proposition 2.4.** *Let  $N$  denote the kernel of (either) projection map  $H \rightarrow \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$ . Then  $N = \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$ , and consequently  $\mathrm{Im} \bar{\rho}_{(E_1, E_2), p} = D_p$ .*

PROOF: Recall that we have a decomposition

$$\mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z}) \simeq \langle \pm I \rangle \times \mathrm{PSL}_2(\mathbf{Z}/p\mathbf{Z}),$$

where  $I$  denotes the identity matrix, and where the projective special linear group  $\mathrm{PSL}_2(\mathbf{Z}/p\mathbf{Z})$  is a simple group since  $p \geq 5$  [1, Proposition 5.1.7]. Thus,  $H$  is determined by a normal subgroup  $N \triangleleft \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$ , and the only possibilities are

$$N \in \left\{ \{I\}, \{\pm I\}, \mathrm{PSL}_2(\mathbf{Z}/p\mathbf{Z}), \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z}) \right\}.$$

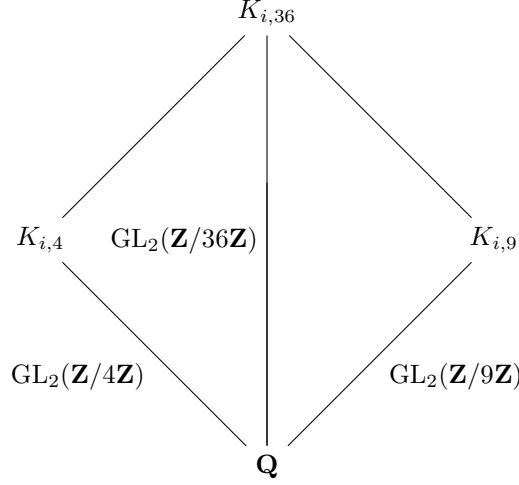
Recall that  $F = K_1 \cap K_2$  and  $F \supset \mathbf{Q}(\zeta_p)$ . By Goursat's lemma and the Galois correspondence, we have that the index  $[\mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z}) : N]$  is equal to the degree of the extension  $[F : \mathbf{Q}(\zeta_p)]$ . Thus we see that  $F$  is strictly larger than  $\mathbf{Q}(\zeta_p)$  if and only if  $N \neq \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$ .

If  $N = \{I\}$ , then in fact  $F = K_1 K_2$ ; this is impossible, as  $\ell_1$  ramifies in  $K_1$  but not in  $K_2$  by Proposition 2.2 and the fact that  $\ell_1 \nmid \Delta(E_2) = \ell_2(432 + \ell_2)$ .

If  $N = \langle \pm I \rangle$ , then  $[K_1 : F] = 2$ . But by Lemma 2.3, the ramification index of  $\ell_1$  in  $K_1/\mathbf{Q}(\zeta_p)$  is bigger than 2, and  $\ell_1$  is unramified in  $K_2$  (and hence in  $F$ ), so this is impossible.

Finally, if  $N = \mathrm{PSL}_2(\mathbf{Z}/p\mathbf{Z})$ , then  $[F : \mathbf{Q}(\zeta_p)] = 2$ , hence  $F/\mathbf{Q}$  is a degree  $2(p-1)$  Galois extension. However, no such Galois subextensions of  $K_1$  or  $K_2$  exist; see the discussion and diagram following [1, Remark 5.2.1].

Thus, the only possibility which our hypotheses allow is  $N = \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$  as desired. ■


 FIGURE 2. Decomposition of the 36-Division Fields for  $E_i$ 

### 3. $p^2$ -DIVISION FIELDS FOR $p = 2, 3$

In this section, we deal with Condition (2) of Lemma 1.9, so given a pair  $(E_1, E_2)$  as before, we now wish to show that

$$(3.1) \quad \text{Im } \bar{\rho}_{(E_1, E_2), 36} = D_{36}.$$

Similar to the setup in Section 2, for  $i = 1, 2$ , let  $K_{i,n} = \mathbf{Q}(E_i[n])$  denote the  $n$ -Division field of  $E_i$ , which is the number field obtained by adjoining to  $\mathbf{Q}$  the  $x$ - and  $y$ -coordinates of the  $n$ -torsion points of  $E_i$ . Since  $E_i$  is a Serre curve, we have

$$\text{Gal}(K_{i,36}/\mathbf{Q}) \simeq \text{GL}_2(\mathbf{Z}/36\mathbf{Z}).$$

Once again, the Weil pairing forces an inclusion  $\mathbf{Q}(\zeta_{36}) \subset K_{i,36}$ , where  $\zeta_{36}$  is a primitive 36-th root of unity. It follows that  $K_{1,36} \cap K_{2,36} \supset \mathbf{Q}(\zeta_{36})$  is a nontrivial extension of  $\mathbf{Q}$ . Just as in the  $p \geq 5$  case, this implies that the Galois group  $\text{Gal}(L/\mathbf{Q})$  of the compositum  $L = K_{1,36}K_{2,36}$  is a *proper* subgroup of  $(\text{GL}_2(\mathbf{Z}/36\mathbf{Z}))^2$ , determined (via Goursat's lemma) by a normal subgroup of  $\text{GL}_2(\mathbf{Z}/36\mathbf{Z})$ . Condition (3.1) is equivalent to the statement that  $K_{1,36}$  and  $K_{2,36}$  are maximally disjoint in the sense that

$$\text{Im } \bar{\rho}_{(E_1, E_2), 36} = D_{36} \iff K_1 \cap K_2 = \mathbf{Q}(\zeta_{36}).$$

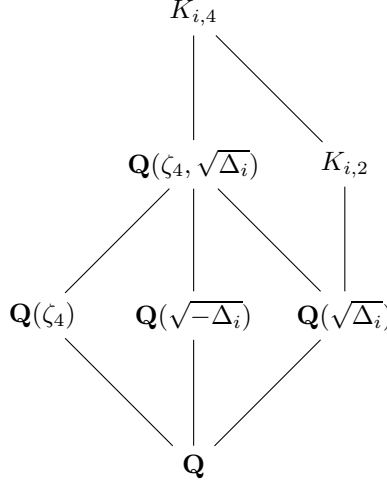
For  $i = 1, 2$  Figure 2 illustrates the decomposition of  $K_{i,36}$  in terms of smaller division fields. The edges are marked by Galois groups, which are determined by the fact that  $E_i$  is a Serre curve.

Noting that  $\text{GL}_2(\mathbf{Z}/36\mathbf{Z}) \simeq \text{GL}_2(\mathbf{Z}/4\mathbf{Z}) \times \text{GL}_2(\mathbf{Z}/9\mathbf{Z})$ , we see that Figure 2 and Goursat's lemma imply that  $K_{i,4} \cap K_{i,9} = \mathbf{Q}$ . Furthermore, since  $\text{Gal}(L/\mathbf{Q})$  is a subgroup of  $\text{Gal}(K_{1,36}/\mathbf{Q}) \times \text{Gal}(K_{2,36}/\mathbf{Q})$ , the same diagram shows that verifying (3.1) is equivalent to verifying the following three assertions:

- $K_{1,4} \cap K_{2,4} = \mathbf{Q}(\zeta_4)$ ;
- $K_{1,9} \cap K_{2,9} = \mathbf{Q}(\zeta_9)$ ;
- $K_{i,4} \cap K_{j,9} = \mathbf{Q}$  for  $i \neq j$ .

We now handle each case in turn. For the rest of the section, let  $\Delta_i = -\ell_i(432\ell_i + 1)$  denote the discriminant of  $E_i$ . Just as in Section 2, our arguments will depend crucially on our hypothesis that  $\gcd(\Delta_1, \Delta_2) = 1$ .

**Lemma 3.1.** *For our pair  $(E_1, E_2)$ , we have  $K_{1,4} \cap K_{2,4} = \mathbf{Q}(\zeta_4)$ .*

FIGURE 3. A portion of the subfield diagram of  $K_{i,4}$  from [1, Figure 5.7]

PROOF: The subfield structure of 4-division fields of elliptic curves is explained in detail in [1, Chapter 5.5]. In particular, every subfield of  $K_{i,4}$  which properly contains  $\mathbf{Q}(\zeta_4)$  also contains  $\mathbf{Q}(\zeta_4, \sqrt{\Delta_i})$ , as well as *all* subfields which are quadratic over  $\mathbf{Q}$ . (See Figure 3.) Let  $F = K_{1,4} \cap K_{2,4}$ , so we have a containment  $\mathbf{Q}(\zeta_4) \subset F$ . By the subfield diagram, if  $[F : \mathbf{Q}(\zeta_4)] > 1$  then we must also have  $\mathbf{Q}(\zeta_4, \sqrt{\Delta_1}) \subset F \subset K_{2,4}$ . But then this implies that the quadratic field  $\mathbf{Q}(\sqrt{\Delta_1})$  is also contained in  $F \subset K_{2,4}$ . However, the only quadratic subfields of  $K_{2,4}$  are

$$\mathbf{Q}(\zeta_4), \mathbf{Q}(\sqrt{\Delta_2}), \text{ and } \mathbf{Q}(\sqrt{-\Delta_2}).$$

Since  $\ell_1$  is an odd prime and  $\gcd(\Delta_1, \Delta_2) = 1$ , we cannot have equality between  $\mathbf{Q}(\sqrt{\Delta_1})$  and any of the aforementioned fields. So we must have  $[F : \mathbf{Q}(\zeta_4)] = 1$  which proves the lemma. ■

The argument for the case of 9-division fields is very similar to that of Lemma 3.1. First we recall a result about the structure of the 3-Division fields of elliptic curves.

**Lemma 3.2.** *Let  $M = \mathbf{Q}(x(E_i[3]))$  denote the number field obtained by adjoining to  $\mathbf{Q}$  the  $x$ -coordinates of the 3-torsion points of  $E_i$ . Then  $\mathbf{Q}(\sqrt[3]{\Delta_i}, \zeta_3)$  is the unique subfield of  $M$  which has degree 6 over  $\mathbf{Q}$ . The only other subfield of  $K_{i,9}$  which has degree 6 over  $\mathbf{Q}$  is  $\mathbf{Q}(\zeta_9)$ .*

PROOF: The first statement is [1, Proposition 5.4.3]. The second statement is visible in [1, Figure 5.4]. ■

**Lemma 3.3.** *For our pair  $(E_1, E_2)$ , we have  $K_{1,9} \cap K_{2,9} = \mathbf{Q}(\zeta_9)$ .*

PROOF: The subfield structure of 9-Division fields of elliptic curves is also explained in detail in [1, Chapter 5.2]. In particular, by [1, Figure 5.4] every subfield of  $K_{i,9}$  which properly contains  $\mathbf{Q}(\zeta_9)$  also contains  $\mathbf{Q}(\zeta_3, x(E_i[3]))$

Let  $F = K_{1,9} \cap K_{2,9}$ , so we have a containment  $\mathbf{Q}(\zeta_9) \subset F$ . If  $[F : \mathbf{Q}(\zeta_9)] > 1$  then we must also have  $\mathbf{Q}(\zeta_3, x(E_1[3])) \subset F \subset K_{2,9}$ . But then Lemma 3.2 implies that

$$\mathbf{Q}(\sqrt[3]{\Delta_1}, \zeta_3) = \mathbf{Q}(\sqrt[3]{\Delta_2}, \zeta_3)$$

which is impossible since  $\gcd(\Delta_1, \Delta_2) = 1$ . Thus  $[F : \mathbf{Q}(\zeta_9)] = 1$  which proves the lemma. ■



It remains to consider the possible entanglement between the 4- and 9-Division fields of our elliptic curves. By symmetry it suffices to show the following.

**Lemma 3.4.** *For our pair  $(E_1, E_2)$ , we have  $K_{1,4} \cap K_{2,9} = \mathbf{Q}$ .*

PROOF: By [1, Figure 5.4], every subextension of  $K_{2,9}$  which is Galois over  $\mathbf{Q}$  contains  $\mathbf{Q}(\zeta_3)$  as the unique subextension which is quadratic over  $\mathbf{Q}$ . Therefore, if  $F = K_{1,4} \cap K_{2,9}$  satisfies  $[F : \mathbf{Q}] > 1$ , then  $\mathbf{Q}(\zeta_3) \subset F$ . But also  $F \subset K_{1,4}$ , and as shown in Figure 3, the only quadratic subextensions of  $K_{1,4}$  are

$$\mathbf{Q}(\zeta_4), \mathbf{Q}(\sqrt{-\Delta_1}), \text{ and } \mathbf{Q}(\sqrt{\Delta_1}).$$

One checks that if  $\ell_1 = 3$  then  $\Delta_1 = 3 \cdot 1297$ ; otherwise,  $\ell_1 > 3$  and  $\nu_{\ell_1}(\Delta_1) = 1$ , so in any case none of these extensions is equal to  $\mathbf{Q}(\zeta_3)$ . It follows that  $[F : \mathbf{Q}] = 1$ , proving the lemma. ■

We summarize the results of this section.

**Proposition 3.5.** *For our chosen pair of elliptic curves  $(E_1, E_2)$ , we have*

$$\text{Im } \bar{\rho}_{(E_1, E_2), 36} = D_{36}$$

PROOF: This follows immediately Lemma 3.1, Lemma 3.3, and Lemma 3.4. ■

We can now prove the main result of this paper.

**Theorem 3.6.** *Let  $\ell_1$  and  $\ell_2$  be odd primes not equal to 7 such that  $\gcd(432\ell_1^2 + \ell_1, 432\ell_2^2 + \ell_2) = 1$ , and for  $i = 1, 2$  let*

$$E_{\ell_i} : y^2 + xy = x^3 + \ell_i.$$

*Then the pair  $(E_{\ell_1}, E_{\ell_2})$  is a Serre pair.*

PROOF: This follows immediately from Lemma 1.9, Proposition 2.4, and Proposition 3.5. ■

#### 4. SERRE $k$ -TUPLES

Given a  $k$ -tuple of elliptic curves  $(E_1, \dots, E_k)$ , one can generalize the above construction in the obvious way to obtain a representation

$$\rho_{(E_1, \dots, E_k)} : G_{\mathbf{Q}} \rightarrow (\text{GL}_2(\widehat{\mathbf{Z}}))^k,$$

whose image is contained in

$$D^{(k)} := \left\{ (A_1, A_2, \dots, A_k) \in (\text{GL}_2(\widehat{\mathbf{Z}}))^k : \det A_1 = \det A_2 = \dots = \det A_k \right\}.$$

Unsurprisingly, one has

$$\left[ D^{(k)} : \text{Im } \rho_{(E_1, \dots, E_k)} \right] \geq 2^k.$$

**Definition 4.1.** For any integer  $k \geq 1$ , a  $k$ -tuple  $(E_1, \dots, E_k)$  of elliptic curves is called a *Serre  $k$ -tuple* if  $[D^{(k)} : \text{Im } \rho_{(E_1, \dots, E_k)}] = 2^k$ .

In [4, Theorem 4.3], it is shown that almost all  $k$ -tuples of elliptic curves are Serre  $k$ -tuples. Theorem 3.6 easily generalizes to the case  $k \geq 2$ .

**Theorem 4.2.** *Let  $\ell_1, \dots, \ell_k$  be odd primes not equal to 7 such that  $\gcd(432\ell_i^2 + \ell_i, 432\ell_j^2 + \ell_j) = 1$  for each pair  $1 \leq i < j \leq k$ . For each  $1 \leq i \leq k$  let*

$$E_{\ell_i} : y^2 + xy = x^3 + \ell_i.$$

*Then  $(E_{\ell_1}, \dots, E_{\ell_k})$  is a Serre  $k$ -tuple.*

PROOF: Just as in the  $k = 2$  case, showing that  $(E_{\ell_1}, \dots, E_{\ell_k})$  is a Serre  $k$ -tuple is equivalent to showing that the  $E_{\ell_i}$  have maximally disjoint division fields [3, Corollary 6.7]. Since the discriminants of each elliptic curve in the  $k$ -tuple are pairwise relatively prime, Theorem 3.6 shows that the division fields for  $E_{\ell_1}, \dots, E_{\ell_k}$  are pairwise maximally disjoint, and the result follows. ■

**Remark 4.3.** The argument in Corollary 1.7, applied inductively, shows that Theorem 4.2 produces infinitely many examples of Serre  $k$ -tuples.

## 5. FINAL REMARKS

Throughout this paper, we have relied on the elliptic curves

$$E_i := y^2 + xy = x^3 + \ell_i$$

to prove Theorem 3.6. However, a careful reading of our arguments reveals that only the following facts about the  $E_i$  were used:

- $E_i$  is a Serre curve, and
- $\Delta_i = \ell_i(432\ell_i + 1)$

It is clearly necessary for the  $E_i$  to be Serre curves, while precise knowledge of the discriminant of  $E_i$  allowed us to compare the ramification of  $\ell_i$  in various division fields. While Theorem 3.6 provides infinitely many explicit examples of Serre  $k$ -tuples, the arguments in this paper actually prove the following more general statement.

**Theorem 5.1.** *Let  $E_1, \dots, E_k$  be elliptic curves with discriminants  $\Delta_1, \dots, \Delta_k$ , respectively. Suppose that each  $E_i$  is a Serre curve, and that for  $i = 1, \dots, k$  there exist odd primes  $\ell_i > 3$  such that*

- $v_{\ell_i}(\Delta_i) \equiv 1 \pmod{2}$ ;
- $E_i$  has split multiplicative reduction at  $\ell_i$ ; and
- $v_{\ell_i}(\Delta_j) = 0$  for  $i \neq j$ .

*Then  $(E_1, \dots, E_k)$  is a Serre  $k$ -tuple.*

## ACKNOWLEDGMENTS

The authors would like to thank Álvaro Lozano-Robledo and Sam Taylor for their helpful discussions throughout the writing process.

## REFERENCES

- [1] C. Adelmann, *The Decomposition of Primes in Torsion Point Fields*, Springer-Verlag, New York, 2001.
- [2] H. Daniels, *An infinite family of Serre curves*, J. Number Theory 155 (2015), 226–247.
- [3] N. Jones,  *$GL_2$ -representations with maximal image*, Math Res. Lett. 22 (2015) no. 3, 803–839.
- [4] N. Jones, *Pairs of elliptic curves with maximal Galois representations*, J. Number Theory 133 (2013), 3381–3393.
- [5] A. Lozano-Robledo and B. Lundell, *Bounds for the torsion of elliptic curves over extensions with bounded ramification*, Int. J. Number Theory 6 (2010), no. 6, 1293–1309.
- [6] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235–265.
- [7] K. Ribet, *Galois Action on Division Points of Abelian Varieties with Real Multiplications*, Amer. J. Math. 98 (1976), no. 3, 751–804.
- [8] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), pp. 259–331.
- [9] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 2nd Edition, New York, 2009.
- [10] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.

(Harris B. Daniels) DEPARTMENT OF MATHEMATICS AMHERST COLLEGE BOX 2239 P.O. 5000 AMHERST, MA 01002-5000

*E-mail address:* `hdaniels@amherst.edu`

(Jeffrey Hatley) DEPARTMENT OF MATHEMATICS BAILEY HALL 202 UNION COLLEGE SCHENECTADY, NY 12308

*E-mail address:* `hatleyj@union.edu`

(James Ricci) DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE DAEMEN COLLEGE DUNS SCOTUS 339 4380 MAIN STREET AMHERST, NY 14226

*E-mail address:* `jricci@daemen.edu`